White Paper

Bloor

Best practices for cloud security

...how security in the cloud can be a better bet than doing it yourself

A White Paper by Bloor Research
Author : Fran Howarth
Publish date : January 2012

Although due diligence is required in the selection of such services, organisations should no longer consider security to be an inhibitor in the use of cloud services

Fran Howarth

Executive summary

The use of cloud-based services is growing rapidly, with the use of software as a service (SaaS), in particular, now becoming mainstream. There are many advantages to be gained through the use of such services rather than deploying and managing technology in-house, and many of those benefits, such as cost savings and flexibility, are well documented. However, as a relatively immature technology delivery mechanism, some originally considered security to be an inhibitor to adoption.

That is something that is changing fast, and many now consider improved security to be among the reasons to subscribe to cloud services. Among the reasons for this is that security can be provided that is often better, cheaper and more effective than that available for in-house deployment—for example, by pushing out mitigation against the very latest threats as they are uncovered to all subscribers automatically. Services are more scalable and are better able to meet modern working demands by extending protection to mobile devices.

Cloud delivery is suitable for a wide range of security services, from basic needs such as malware protection to advanced security services such as vulnerability management, security monitoring, policy compliance, and application security and testing. As well as accessing security services, organisations will also benefit from the service provider taking responsibility for many aspects of security as it must itself have developed a highly secure infrastructure in line with best practice and good governance objectives. These incorporate a wide range of security controls and can attest to the quality and security of its services through management reports and audit trails.

This document discusses how cloud-based security services can benefit organisations of all sizes. However, there are still some issues and challenges that remain to be ironed out. This document aims to provide advice to organisations as to what they should look for when considering cloud-based services and what pitfalls there are to avoid.

Fast facts

- Cloud-based security can be more robust, effective and cheaper than technology deployed and managed in-house.
- Security is increasingly being seen as a driver, rather than an inhibitor, to the take up of cloud-based services.
- Issues and challenges that remain include liability, contracting and SLA terms and conditions, data centre infrastructure, auditing and certification, and the need for further standards development.

The bottom line

Ensuring that networks are secure and that compliance with regulations and industry standards can be achieved is a complex task for any organisation no matter how small or large. An organisation that tries to do everything itself will be in a constant state of catch up, which often leaves vulnerabilities exposed. As networks become increasingly open and inter-connected, with always-on availability expected from an ever-growing variety of devices, a far better strategy is to offload security needs that are either not a core competence or that are complex and costly to manage to a third party that has specialised expertise.

Cloud services showing strong levels of growth

Statistics regarding cloud computing vary widely, but there is one thing they all have in common—growth rates are strong; in fact more so than for any other area of IT spending. According to a recent report by the Boston Consulting Group, enterprise cloud computing will account for 10% of the global IT services and enterprise software market in 2012. Cloud computing can take many forms, including private and public clouds, the use of cloud computing for network infrastructure and computing platform needs, or for subscribing to hosted applications. Of these, the latter is the most popular, commonly referred to as software as a service (SaaS).

There are many benefits to be derived from cloud computing. Organisational networks have become increasingly complex over the past couple of decades and now encompass a multitude of applications, hardware to run those applications and peripherals such as communications equipment. In the traditional on-premise technology delivery model, all systems must be provisioned individually, applications installed on devices, including patches and updates, and configurations managed to ensure everything is working as it should and there are no vulnerabilities that could be exploited. That is a time-consuming task that requires a lot on the part of IT administrators.

In the SaaS model, applications are provisioned centrally and are accessed through an internet browser without the need to install software on every device that is used to access those applications. Among the most cited benefits that this brings are increased scalability; cost savings in terms of software licences, hardware and maintenance; and ease of management. SaaS also caters to the demands of today's always-on generation for accessing information whenever they want from wherever they are, and especially through mobile devices that have internet access. According to the International Telecommunications Union, there were 5.9 billion mobile cellular subscriptions in 2011, up from 738 million in 2000, and an increasing proportion are so-called smartphones that provide internet access. More recently, tablet computer sales have really taken off with the release of new models and high levels of growth are expected to continue.

Cloud services can improve security

Many organisations have shown some level of reluctance over embracing cloud computing, with security cited as one of the primary concerns. In many cases, subscribing to cloud-based SaaS services means that an organisation must cede control over the processing and storage of its business information, much of which is sensitive and subject to regulatory demands and that it be handled in a secure manner at all times. Because of this, many surveys point to data confidentiality and privacy as prime concerns in the use of cloud-based services.

Confidentiality is one of the three pillars of the traditional information security model, along with availability and integrity. All three pillars are concerns voiced by organisations regarding the use of cloud computing and are key factors in the selection of a cloud service provider. In terms of availability, cloud services can be provided on a 24x7 basis and cloud services providers invest heavily in business continuity and disaster recovery capabilities, providing guarantees over data recoverability and the uptime of the service. Confidentiality can be assured by security controls such as those placed over access rights, the use of strong authentication methods, and encryption for data both when in transit and at rest. For ensuring the integrity of data, tools can be used to prove that no data has been altered, which is backed up by management reports and audit trails of all actions taken.

The information in Table 1 is provided by ENISA, the European Network and Information Security Agency. It outlines the way that responsibility for security should be divided between the customer and the provider of the service. This information refers primarily to the division of responsibilities for SaaS offerings, where more of the security requirements are delegated to the service provider than for platform- or infrastructure-as-a-service offerings.

Customer	Service Provider
• Compliance with data protection laws in terms of the data that it collects and processes • Maintenance and manageability of identity management system and authentication platform	• Physical infrastructure security and availability • Patch management and hardening procedures • Security platform configuration • Systems monitoring • Security platform maintenance • Log collection and security monitoring

Table 1: Division of responsibility for SaaS offerings Source: ENISA

With such controls in place by service providers to ensure that the infrastructure is secure and that data and applications are adequately and securely protected, cloud computing can actually improve security. The recently published 2011 Cloud Computing Outlook Survey by Cloud.com found mixed feelings among respondents with regard to perceptions of security. Of 521 respondents, 36% stated that security is a factor that is inhibiting their use of cloud computing, yet 32% stated that security is a factor influencing their choice to use cloud computing. For many years, large organisations have used IT service providers to help them keep their technology assets in good shape; now even the smallest of firms are making use of cloud-based services in larger numbers, not just to save costs but also to improve their security posture and capabilities.

Some of the ways in which cloud computing can improve security are discussed below.

Security can be cheaper and more effective

Cloud architecture
Governance and enterprise risk
Legal and electronic discovery
Compliance and audit
Information lifecycle management
Portability and interoperability
Traditional security, business continuity management and disaster recovery
Data centre operations
Incident response
Application security
Encryption and key management
Identity and access management
Virtualisation

Table 2: Security domains for cloud computing Source: Cloud Security Alliance

Whilst much early adoption of SaaS services was for access to enterprise business applications, such as customer relationship management and payroll administration, organisations are increasingly looking to the cloud to access security applications that they would previously have implemented and managed in-house. Organisations of all sizes are increasingly being targeted by hacker and malware attacks, and these are becoming more complex and sophisticated, and therefore harder to defend against. Attacks now commonly use blended threat vectors, such as combining a phishing email with a link to a malware-riddled website, or one that has been misappropriated or spoofed.

Because of factors such as these, organisations are increasingly looking beyond the use of the cloud for business applications that improve productivity, such as those mentioned above, to the use of security services offered by cloud providers. With cloud computing, security can be implemented on a large scale and in a uniform, more effective manner across the organisation, including support for all mobile devices, with all services managed through one centralised interface. This provides for security policies to be defined and enforced, and for detailed reports of all activity to be provided to customers for audit and control purposes.

With traditional, on-premise technology delivery models, organisations need to deploy and manage software licences and the hardware to house them themselves, as well as upgrading all user devices with the latest updates and patches. That process has to be repeated with each instance of software. In even a fairly small organisation this can be a huge task, owing to the complexity of most networks in terms of the number of systems that they contain and applications that run on them, and this may lead to some systems going unpatched. Even where patches and updates are performed in a uniform and timely manner, patch installation, adjustments to communications settings or software updates can cause configurations to be changed, which can lead to security risks being introduced that could expose vulnerabilities that can be exploited.

Security can be cheaper and more effective

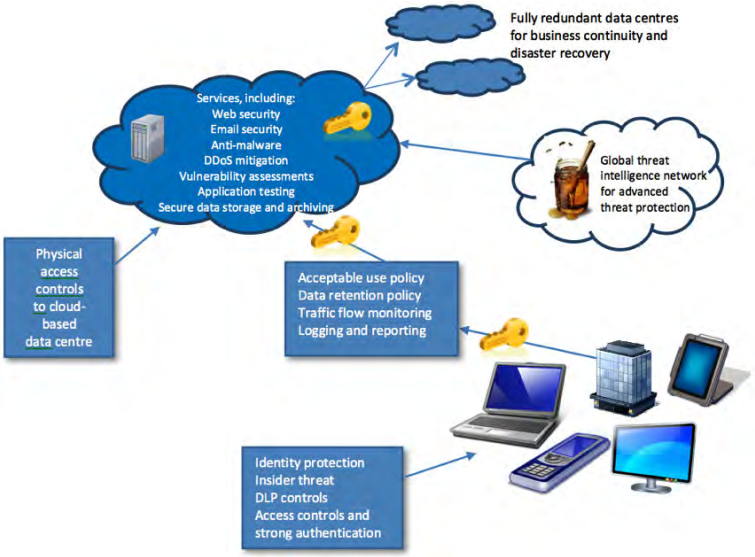

Figure 1: Selected security services in the cloud

Configuration errors are a major cause of network downtime and vulnerabilities and are a drain on the time of IT administrators. There is often little time left over to check configurations after each change has been made or to carry out preventative maintenance—especially for organisations that lack sufficient IT or dedicated security resources. For many, the challenges of ensuring that vulnerability assessments and remediation are performed, or that policies for systems such as firewalls are updated in a timely manner, are too much for the organisation and security flaws accumulate over time. As a result, security incidents can multiply and regulatory compliance objectives go unmet.

As shown in Table 1, the use of cloud computing services pushes much of the burden of security onto the service provider. To ensure that the services that it offers are secure, the integrity and confidentiality of the information being processed and stored is maintained, and are always available, any cloud provider needs to establish a secure, hardened IT infrastructure that will aid organisations in their application and data resilience strategies and which will allay many fears over data security. This infrastructure must also be developed in accordance with proper governance guidelines and a best practices framework, taking into account prevalent security regulations and industry standards such as data protection and PCI. Given the complexity of the regulations and standards with which organisations must adhere, this can be a great help in reducing the burden of regulatory compliance—as well as providing the ability to prove that compliance objectives are being met through reports and audit trails provided by the service provider that demonstrate the effectiveness of the controls they have in place.

The cloud is also an ideal way for organisations to gain access to more advanced security services above and beyond those such as malware protection services and secure archiving. These can include scanning and monitoring of activity for vulnerabilities, including ensuring that external facing assets such as e-commerce sites are secure and available. Included in this can be capabilities such as monitoring traffic flow and bandwidth for such exploits as distributed denial of service (DDoS)

Security can be cheaper and more effective

attacks that aim at making such services unavailable. There are some services available that will mitigate such DDoS attacks in the cloud, preventing the traffic from reaching the intended target and overwhelming it.

There are other essential services that can be provided in the cloud that can often be more cost-effective than managing those processes in-house. Few organisations do a good job at log management, especially given the sheer volume of logs that are generated, including network, operating systems, firewalls, anti-malware controls, IDS/IPS and application logs. A cloud service provider can monitor and analyse logs on a 24x7 basis and can provide the results as reports for audit and forensic investigation purposes. These can be turned into actionable data that can be used to detect and protect the organisation against security incidents.

Disaster recovery and business continuity are also services that can be better done by a cloud service provider than managed in-house, especially for smaller organisations. Performed in-house, organisations need to invest in spare hardware and devote resources to its maintenance and recovery in the event of a failure. Through the use of cloud-based services, disaster recovery and business continuity processes can be handed off to the provider, who will guarantee that it has sufficient backup data centre resources and processes in place for failover in the event of an outage. Organisations should look carefully at the service provider's track record in this area, especially given the recent publicised outages by major public cloud vendors that include Google and Microsoft.

Checklist: Critical security controls

☐	Inventory of authorised and unauthorised hardware
☐	Inventory of authorised and unauthorised software
☐	Secure configurations for hardware and software
☐	Secure configurations for network devices such as firewalls, routers & switches
☐	Boundary defence
☐	Maintenance, monitoring and analysis of security logs
☐	Application software security
☐	Controlled use of administrative privileges
☐	Controlled access based on need to know
☐	Continuous vulnerability assessment and remediation
☐	Account monitoring and control
☐	Malware defences
☐	Limitation and control of network ports, protocols and services
☐	Wireless device control
☐	Data loss prevention
☐	Secure network engineering
☐	Penetration tests and red team exercises
☐	Incident responsibility
☐	Data recovery capability
☐	Security skills assessment and appropriate training to fill gaps

Source: SANS Institute: 20 critical security controls, version 3

Remaining challenges and issues

Notwithstanding the many ways that the use of cloud computing can bring security benefits to organisations, many remain sceptical, as shown in Figure 2, which is based on a survey of 300 end-user organisations, the majority of which are based in the UK, that was published in October 2011. In particular, data security and privacy are cited as the main concerns for organisations in subscribing to cloud services.

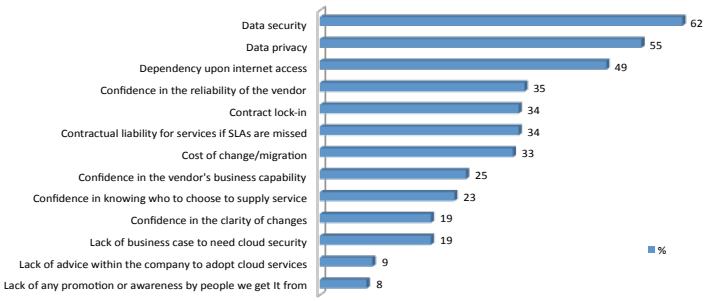

Figure 2: Most significant concerns about cloud adoption Source: Cloud Industry Forum

Liability, contracts and SLAs

A key concern related to data security is which party accepts liability for security incidents such as data breaches. However, many cloud service providers expressly exclude or limit their liability for damage under the terms and conditions of the agreements that they offer. For example, section 11, "Limitations of Liability", of Amazon Web Services customer agreement (November 2011) states:

"We and our affiliates or licensors will not be liable to you for any direct, indirect, incidental, special, consequential or exemplary damages (including damages for loss of profits, goodwill, use or data), even if a party has been advised of the possibility of such damages."

Further, the agreement specifically excludes any responsibility for any compensation, reimbursement or damages arising in connection with any unauthorised access to, alteration of, or the deletion, destruction, damage, loss or failure to store any of the customer's content or other data, with any liability limited to the amount the customer actually pays for the service.

According to recent research conducted by the Cloud Industry Forum among 450 organisations in the UK in 2011, 34% of respondents reported that their cloud service provider excludes liability for data loss in their contracts, and a further 37% of respondents were unsure of the answer.

However, this is an issue that the EU is looking to address alongside changes being made to data protection laws, which look set to include mandatory data breach notification. The EU's Binding Safe Processor Rules is likely to be set up as an accreditation scheme, whereby cloud service providers must prove that their security models are adequate and will accept liability for any data breaches or losses that occur at their data centres. In general, liability will be limited to the cost of the service. According to the Cloud Industry Forum survey, 43% of respondents have taken out specific insurance in the event of any interruption to their business should a disaster occur.

Remaining challenges and issues

The ability to negotiate contracts and SLAs is another area in which organisations are expressing concerns. According to the Cloud Industry Forum, 80% of organisations using cloud services would like more than just a standard contract issued to all customers, but 45% indicated that they were not offered the opportunity to negotiate the terms of the contract. Of those that have been given the opportunity to negotiate terms, they were primarily large organisations. Further, 32% of respondents reported that their cloud service providers could make changes to their contract simply by posting a new version online, and a further 38% indicated that they were not sure about this.

Any contract taken out needs to be accompanied by an SLA that states the specific parameters of the service and the minimum service levels that will be provided for each element of the service. Factors to consider include uptime, where the SLA will specify a guaranteed level of uptime, such as 99.9%. However, organisations need to consider how uptime is measured and what is included in guarantees. For example, scheduled downtime for maintenance where customers have been given a specified period of notice, such as five days, will generally be excluded and some include clauses for service failures that are outside of the control of the service provider. Organisations should look for a service provider that publishes its uptime records, along with other metrics, to see historic performance, and should consider demanding the right to audit performance records and service quality statistics. Where uptime guarantees are not met, customers are generally offered a service credit as compensation, although many providers require the customer to specifically request this within an agreed timeframe.

Other factors to consider include those related to data processing and storage. The contract should specify that data remains the property of the customer and SLAs should state a customer's right to access its data on an ongoing basis as well as in emergency situations. The SLA should also state within what time period data will be returned to a customer both when requested and on termination of the contact. To avoid vendor lock-in through data being only accessible in a proprietary format used only by the service provider, the form in which data will be returned should also be specified. The contract should also specify in what geographical location data will be processed and stored and should specify obligations for data breach notification, including how and when customers will be notified and who is responsible for damages, fines and corrective action. The contract should also specify the security controls and processes that are in place to prevent security incidents from occurring in the first place, such as business continuity, encryption, firewalls, physical security and application security.

Data centre infrastructure

The location and number of the data centres used by any service provider is a key factor when considering subscribing to cloud services. Data centres need to be in locations that are suitable for a customer's needs for data to be processed and stored in an appropriate location to satisfy regulatory compliance needs. For example, data protection laws in the EU prohibit the transfer of personal data to countries without the same level of safeguards over data privacy, and some are even more prohibitive than that, requiring that certain categories of data must not be transferred outside national borders.

However, it is not just the location of the data centre that must be taken into account, but also the country in which the service provider that owns those data centres is located. This is because of issues concerning the use of the Patriot Act and other intelligence-gathering legislation from the US in particular, which can be used to compel organisations to hand over information to the US government. In many cases, such requests are accompanied by a gagging order that prevents the recipient of the request from disclosing that the order has been issued, meaning that organisations may not even be aware that these instruments are being used against them. If the hosting company is a wholly owned US company, it and its subsidiaries in foreign countries are subject to the Patriot Act throughout its operations.

Some service providers have obtained Safe Harbor certifications that provide privacy protections that are designed to meet EU adequacy standards when transferring personal data outside of the EU for processing and reviewing without obtaining the data subjects' consent. However, a number of countries, including the UK, Australia, Canada, the Netherlands, France and Norway, have put in place blocking statutes that prohibit the gathering of business-related information to be used in

Remaining challenges and issues

litigation and that provide for prison sentences, fines or both for transgressions. According to lawyers, such blocking statutes should be interpreted as preventing the formal collection by US courts of any documents, testimony or information from nationals of those countries. However, US case law has determined that sanctions, such as contempt of court, can be imposed by US courts for failure to comply with requests for information. Recipients of such orders must therefore face a choice of breaking national laws or provoking the wrath of US courts.

Organisations should therefore look closely at who actually owns the data centre infrastructure to be used. This is particularly important as some large public cloud providers have stated that they will comply with requests such as those under the Patriot Act and will not inform their customers if there is a gagging order with the request, whilst others have let it be known that they have actually already done so. Recently, the Canadian government has stated that it has a policy of forbidding public-sector IT projects from using US-based hosting services, and the German and Dutch governments are considering similar edicts.

Because of these issues, organisations should look for a provider that has local infrastructure to mitigate concerns over storing data in an offsite location and should scrutinise the terms and conditions of the service to ensure that hosted data is secure and will reside only in data centres within the EU, including secondary data centres for geo-redundancy. They should also seek assurances from the service provider that the procedures for dealing with such requests are tight, with only a limited number of people within the organisation provided with the means to comply so that due consideration will be given to the validity of the request before data is handed over.

When looking at the provider's data centre infrastructure, the number of data centres plays a role as well as their location. A key role played by cloud service providers is in providing disaster recovery and business continuity services, and it is therefore important that it has adequate data centre coverage to ensure failover services and to ensure that a secure backup of all data is available in a separate data centre location, albeit not in a separate jurisdiction in most cases. Organisations should ask what processes the provider has in place for business continuity and disaster recovery and should look at their track records, especially of outages, which have recently plagued some of the large cloud vendors and rendered their services unavailable.

Data centre audits and certification

Before subscribing to a cloud service, organisations should ask the service provider to demonstrate that it has been through an audit of its control objectives and activities. Such audits should be conducted by a qualified, independent third party and should be repeated on an annual basis. Of vital importance, however, is that organisations know what controls and processes are included in the audit. Many service providers aim to achieve certifications such as those in the ISO 27000 group or SAS 70 Type II, which was developed by the American Institute of Certified Public Accountants (AICPA). SAS 70 has increased greatly in popularity since the passing of the Sarbanes-Oxley regulation as SAS 70 audits are identified in that regulation as being the only acceptable method for a third party to assure a service organisation's controls. However, SAS 70 was really designed for audits of financial and transaction reporting and is really just a generic guideline for audits that places the onus on the service recipient to ensure that the controls being audited are relevant. Even though SAS 70 Type II includes an onsite evaluation, it is not proof in itself that the service offered is secure. Because of the lack of specificity over controls for service organisations included in SAS 70, AICPA has developed the Statements on Standards for Attestation Engagements No. 16 (SSAE 16) certification, effective as of June 2011, which includes best practice criteria for assessing the controls of service organisations that perform outsourced services. SSAE 16 has been designed to be in line with the new International Standards on Assurance Engagements (ISAE 3402) international service organisation reporting standards.

Many service providers will also be audited for their compliance with various government regulations and industry standards, such as PCI and Sarbanes-Oxley, with which many of their customers must comply. Organisations should check before signing up for a service that their needs are adequately covered, especially with regard to regulations such as these and those governing the specific geographic region in which they operate.

Remaining challenges and issues

Standards

One area in which further development is needed is that of standards for cloud computing services. As shown in Figure 2, contract or vendor lock-in are considered to be significant concerns regarding the use of such services owing to concerns regarding the interoperability of various cloud services. For example, some cloud services use proprietary formats for processing and storing data, leading to the fear that the data will be unusable if removed from the application, thus preventing an organisation from transferring to another service provider should it wish, or of being unable to retrieve its stored data if the service provider goes out of business. According to the Institute of Electrical and Electronic Engineers, the near future evolution of cloud computing is hypothesized in three subsequent stages: (1) "Monolithic" (now), in which cloud services are based on independent proprietary architectures; (2) "Vertical supply chain", in which cloud providers will leverage cloud services from other providers; and (3) "Horizontal federation", in which smaller, medium and large cloud providers will federate themselves to gain economies of scale and an enlargement of their capabilities.

Another area where standards are lacking is in identity, entitlement and access management for services based in the cloud. To address this issue, the Open Group Jericho Forum, an industry forum working in the areas of security and open networking, published its Identity, Entitlement and Access (IdEA) Commandments in May 2011 that focus on the fundamental design issues surrounding identity management and access to systems, services and data. According to the Jericho Forum, these commandments represent a set of open and interoperable principles that IT professionals can use to build a user-centric security framework within their organisations. Freely available from the Jericho Forum website, the commandments separate identity management and identity access from each other to promote a more effective risk-based approach, with the core principle being that essential personal data stays with the individual to greatly reduce the risk of the information being compromised.

What legal system does the agreement claim to be governed by and are there any limits on where, how or when a legal claim can be brought against the provider?
Does the provider assert the right to vary the contract unilaterally? If so, what, if any, mechanism is there to notify customers?
Are there any undertakings or disclaimers regarding the security of customer data?
What, if any, notice will the provider give regarding deletion of customer data?
On what grounds will the provider disclose customer data to a third party?
What causes of service outage are covered by the SLA? What is the form and level of compensation?
Does the provider exclude or limit liability for damage under the agreement, particularly consequential damages such as business losses?

Table 3: Issues to consider when selecting a cloud services provider Source: The Brookings Institution

Summary

Almost every organisation, whatever its size or line of business, is dependent on technology, but those networks face a barrage of increasingly sophisticated attacks from criminals looking to compromise the sensitive information that they contain. In the physical world we have long relied on specialist services such as the police for providing security. In terms of information security, many large enterprises have commonly used the services of specialised contractors and service providers. In the age of cloud computing, those services are available to organisations of any size and make enterprise-grade security available to even the smallest organisation. They are also more suitable to the modern era of always-on technology access, where mobile connectivity and online interaction are the norm. Although due diligence is required in the selection of such services, organisations should no longer consider security to be an inhibitor in the use of cloud services, but rather should embrace them for the benefits that they can bring in terms of reduced risk, improved security and the ability to more easily achieve governance and compliance objectives.

Further Information

Further information about this subject is available from
http://www.BloorResearch.com/update/2121

Bloor Research overview

Bloor Research is one of Europe's leading IT research, analysis and consultancy organisations. We explain how to bring greater Agility to corporate IT systems through the effective governance, management and leverage of Information. We have built a reputation for 'telling the right story' with independent, intelligent, well-articulated communications content and publications on all aspects of the ICT industry. We believe the objective of telling the right story is to:

- Describe the technology in context to its business value and the other systems and processes it interacts with.
- Understand how new and innovative technologies fit in with existing ICT investments.
- Look at the whole market and explain all the solutions available and how they can be more effectively evaluated.
- Filter "noise" and make it easier to find the additional information or news that supports both investment and implementation.
- Ensure all our content is available through the most appropriate channel.

Founded in 1989, we have spent over two decades distributing research and analysis to IT user and vendor organisations throughout the world via online subscriptions, tailored research services, events and consultancy projects. We are committed to turning our knowledge into business value for you.

About the author

Fran Howarth
Senior Analyst - Security

Fran Howarth specialises in the field of security, primarily information security, but with a keen interest in physical security and how the two are converging. Fran's other main areas of interest are new delivery models, such as cloud computing, information governance, web, network and application security, identity and access management, and encryption.

Fran focuses on the business needs for security technologies, looking at the benefits they gain from their use and how organisations can defend themselves against the threats that they face in an ever-changing landscape.

For more than 20 years, Fran has worked in an advisory capacity as an analyst, consultant and writer. She writes regularly for a number of publications, including Silicon, Computer Weekly, Computer Reseller News, IT-Analysis and Computing Magazine. Fran is also a regular contributor to Security Management Practices of the Faulkner Information Services division of InfoToday.

Copyright & disclaimer

2nd Floor,
145–157 St John Street
LONDON,
EC1V 4PY, United Kingdom

Tel: +44 (0)207 043 9750
Fax: +44 (0)207 043 9748
Web: www.BloorResearch.com
email: info@BloorResearch.com